RECEIVED
CENTRAL FAX CENTER
NOV 17 2006

REMARKS

1. Applicant thanks the Examiner for her remarks and observations which have greatly assisted Applicant in responding.

2. **35 U.S.C. § 112**

Claims 29-33, 66-70, 78-82, 88-91 and 94 stand rejected under 35 U.S.C. § 112, 2nd paragraph as being indefinite for failing to distinctly claim and particularly point out the subject matter of the invention.

Claims 29, 32-33, 66-67, 78, 80-82 and 90 are found to be indefinite because they contain the term "configurable" which is allegedly a relative term. Applicant respectfully disagrees. The term "configurable" is widely understood in the present context among ordinarily-skilled artisans to mean that a parameter can be set or specified. The term is used throughout the specification, and the ordinarily-skilled artisan would readily understood that it is used to indicate that the expression modified by the term "configurable" refers to an element, or a parameter or a setting that can be specified or set. Even though Applicant disagrees with the present finding, in the interest of advancing prosecution of the Application, the claims have been amended to substitute the term "specified" for the allegedly offending term "configurable."

Claims 79-80 are found to be indefinite because the expression "trusted address range" is allegedly indefinite. The Examiner finds that neither the claims nor the specification define the term "trusted." Applicant respectfully disagrees. United States published application no. 2005/0108551 defines a trusted entity as a user ID/client pair from which a successful login has been made (¶ 0023). ¶¶ 0094-0109 describe the process by which trust is extended to a user ID/address pair when the client is an anonymous client that cannot be uniquely identified. It is apparent from the description that a trusted address is an address from which a user has successfully logged in. It is also apparent from the description that a "trusted address range" is a range of addresses defined by the addresses from which the user has previously successfully logged on. Accordingly, the

finding that the term trusted is not defined in the specification is incorrect. Because the ordinarily-skilled practitioner, by referring to the specification, would readily understand the term, the present rejection is deemed improper. Nevertheless, in the interest of advancing prosecution of the application, Applicant amends claim 79 to describe "determining a trusted address range, defined by client IP addresses from which successful authentications have originated . . .." Because the claims as amended explicitly define the trusted address range, the present amendment would overcome the present rejection if it were not improper.

Claim 81 has been amended to describe a "trusted address range." Therefore the present rejection is deemed overcome.

2. **35 U.S.C. § 101**

Claims 38-74 stand rejected as being directed to non-statutory subject matter because they are alleged not to produce a useful or tangible result. Claim 38 has been amended to describe "processing remaining requests according to at least a second policy so that untrusted network traffic is limited." Limiting untrusted network traffic is a useful result because it helps to alleviate problems for users and Internet service providers caused by security breaches such as systematic password theft and cracking software. Because claim 38 as amended describes a useful result, the present rejection is deemed overcome.

3. **35 U.S.C. § 102**

Claims 1-8, 38-45, 11-28, 30-31, 35, 48-65, 67-68 and 72 stand rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. published application no. 2003/0046533 ("Olkin"). Applicant respectfully disagrees. Applicant notes that the Examiner has provided no explanation of how she has applied the cited teachings to the claims, rendering it necessary for Applicant to guess at her rationale.

The Examiner relies on Olkin ¶ 0045 as teaching "identifying entities legitimately entitled to service; " and "establishing said identified entities as

trusted entities." As described in ¶ 0045, the sender of a secure email authenticates on the security server and the security server provides the sender with a message key and ID for the message being sent.

The Examiner next relies ¶¶ 0045 and 0046 as teaching

"processing requests from said trusted entities according to a first policy; and

processing remaining requests according to at least a second policy."

While it does appear that requests from the sender are processed according to a first policy, as described in lines 1-9 of ¶ 0046, wherein the sender's message is delivered to a registered recipient and the sender's message is only delivered to an unregistered recipient after the unregistered recipient registers, the Examiner points to no teaching from Olkin describing a second policy for treatment of messages sent by untrusted senders. Accordingly, the present rejection is deemed to be improper.

In spite of the foregoing, in order to describe the invention more clearly, Applicant amends claim 1 to describe:

identifying entities legitimately entitled to service, wherein an entity comprises a user ID/client pair;

establishing said identified entities as trusted entities by issuing a trust token for each entity successfully authenticating to said network service, said trust token comprising a data object that includes a client identifier;

processing requests from said trusted entities according to a first policy; and

processing remaining requests according to at least a second policy. "

As amended, claim 1 incorporates the subject matter of claims 2, 6, 7 and 11. Claim 38 is similarly amended, incorporating the subject matter of claims 39, 43, 44 and 48.

While Applicant acknowledges that claims 2, 6, 7,11, 39, 43, 44 and 48 presently stand rejected, the rejection of these claims, as applicant demonstrates below is improper

Claims 2 and 39: The Examiner relies on Olkin ¶ 0079 as teaching "wherein an entity comprises a user ID/client pair." Applicant respectfully disagrees. ¶ 0079 describes the contents of the tables shown in figs. 6a-d. However, in examining figs. 6a-d, while Applicant does find UserId and password to uniquely identify the user, Applicant finds no means whatsoever of uniquely specifying the client that the user is using. Fig. 6a is a basic user information table; fig. 6b is a 'sent messages' table; fig. 6c is an 'email destinations' table; and 6d is an 'an alternate user identities' table. Not a word is said about the client. The Examiner may say that the message key identifies the client; such assertion would be incorrect because the key is associated to the message, and the very same key is transmitted to the recipient in order to decrypt the message.

The Examiner may also say that the email address identifies the client. The Examiner would also be incorrect here because a user can send and receive emails through his or her email account via any client with which the user can access the account, so that the email address is only associated to the user, not to a particular client. Thus, the email address would not suffice to identify a particular client.

Accordingly, the Examiner has not identified a teaching from Olkin that teaches the subject matter of claims 2 and 39. The rejection of claims 2 and 39 as being anticipated by Olkin is therefore improper.

Claims 6 and 43: The Examiner relies on Olkin ¶ 0079 as teaching "wherein establishing said identified entities as trusted entities comprises the step of: issuing a trust token for each entity successfully authenticating to said network service." There is no teaching whatsoever in the cited paragraph of issuing a trust token to an entity successfully authenticating to said network service." The cited paragraph describes the user registration process, wherein authentication

credentials are issued to a user who has just registered. Because authentication credentials, as described in ¶¶ 0045 and 0046, are required in order to authenticate successfully, a newly-registered user who has just been issued authentication credentials cannot possibly have authenticated successfully.

Claims 7 and 44: The Examiner relies on Olkin ¶ 0049 as teaching "wherein said trust token comprises a data object." While the cited paragraph does teach that the security server sends the client a message ID and a message key, which are data objects, the data objects in question are not trust tokens. They are associated to the message and serve only to identify the message and to decrypt it and they do not identify the client as a trusted client. As Applicant has previously explained, there is no teaching anywhere in Olkin of anything that can be reasonably found to teach a client identifier.

Claims 11 and 48: The Examiner relies on Olkin, ¶ 0075 as teaching "said data object including a client identifier." Applicant respectfully disagrees. The cited paragraph describes the user aliases table which includes fields for email address and UserId –neither having anything to do with identifying the client. While, in the absence of any explanation of how the claims are alleged to read on the cited paragraphs, it is difficult to guess, Applicant surmises that the Examiner finds the email address to be equivalent to a "client identifier." However, because an email address is associated to a user, it could be said to be a user identifier; however, an email address it not associated to a particular client. In fact, an email address is not really an address at all, but rather the name of an email account that is hosted on a particular domain server. Additionally, the Examiner is certainly well aware that messages associated to a particular email address (account) can originate from any client from which the user can access his or her email account. Accordingly, there is no teaching in claims 11 and 48 of "the data object including a client identifier."

Because amended claims 1 and 38 incorporate subject matter not taught by Olkin, the present amendment overcome the rejection of claims 1 and 38.

Even if the present amendment had not been made the rejection of claims 1 and 38 is improper and there fore the claims would be allowable.

In view of their dependence from allowable parent claims, the dependents are deemed allowable without any separate consideration of their merits. Nevertheless, Applicant has the following comments regarding the dependent claims:

Claims 8 and 45: The Examiner relies on Olkin ¶ 0049 as teaching: "said data object including: said user ID or a derivative thereof." The data object transmitted to the receiver includes only the message ID and the key. There is no transmission by the security server to the receiver unit of the user ID or a derivative thereof.

Claims 12 and 49: The above remarks regarding claims 11 and 48 are equally applicable here.

Claims 13 and 50: The Examiner relies on Olkin, ¶ 0074 as teaching "encrypting said trust token." While the cited paragraph describes storage of the user's password on the server as a hash, there is no teaching at all that a trust token is encrypted.

Claims 14 and 51: The Examiner relies on Olkin, ¶ 0115 as teaching "transmitting said trust token from said network service to said client upon successful authentication to said network service by said entity." Applicant respectfully disagrees. The cited paragraph has nothing to do with transmission of a trust token. What is described is the generation of a message ID, a message and set of seals for the various portions of the email to be sent. Nothing at all is transmitted in this paragraph, let alone a trust token.

Claims 17 and 54: The Examiner relies on Olkin, ¶ 0095 as teaching storing said issued trust token on said client. The cited paragraph has nothing to do with

storing a trust token on the client. What is described is the storage by the client application of a user password. However, the user password is associated only to the user, not to the client. Applicant also notes that claims 17 and 54 depend from claims 7 and 44. In her comments regarding claims 7 and 44, the Examiner found that message ID and the message Key constituted a trust token. It can't be both, and in fact it can't be either, because the message key and message ID are only associated to the message, not to the client.

Claims 18 and 55: The Examiner relies on Olkin, ¶ 0095 as teaching "transmitting said stored issued trust token along with said user ID, authentication credentials, and client identifier from said client to said network service." What is described in ¶ 0095 is the 'sent mail' table from fig. 6b. While the table does include a UserID, there is no evidence of authentication credentials, or of a trust token or of a client ID. In view of the amendment to the parent claims, mention of the "client identifier" has been eliminated from these claims.

Claims 19 and 56: The Examiner relies on Olkin, ¶ 0085 as teaching transmitting said stored, issued trust token occurs via a secured channel." While the cited paragraph does mention transmission via SSL, the transmission is not of a trust token associated to the client, but of a message ID and a message key.

Claims 21 and 58: The Examiner relies on Olkin, ¶¶ 0074-0075 as teaching "storing said issued trust token in a server side database, indexed according to a combination of user ID and client identifier." The cited paragraphs describe the 'users' table and the 'user aliases' table. There is no teaching in the cited paragraphs of a trust token or indexing a trust token by one or both of UserId or client identifier. Applicant cannot guess where in the cited paragraphs the teaching of a "trust token" is found and respectfully requests additional guidance. It appears that the Examiner again finds that an email address is equivalent to a client ID. As previously explained, an email address and a client ID are two

completely different entities that cannot be made to read on each other in the context of the invention.

Claims 22 and 59: The Examiner relies on Olkin, ¶¶ 0103-0109 as teaching "transmitting said client identifier assigned by said network service from said network service to said client upon successful authentication to said network service by said entity." First, there is no teaching in the cited paragraphs of anything being transmitted from the network service to the client. The objects being transmitted are going from the client to the server. It does appear that the client is authenticating on the server because authentication credentials are transmitted. Otherwise, there is no mention of a client identifier being transmitted in either direction. In addition to the authentication credentials, only the sender email address, recipient addresses, the encrypted message, the unencrypted subject field and optional configuration information are transmitted.

Claims 25 and 62: The Examiner relies on Olkin, ¶ 0114 as teaching "transmitting said user ID and client identifier to said server; and retrieving said stored trust token from said database." The cited paragraph does mention that the sender is considered authenticated. Thus, the sender must have sent authentication credentials. However, otherwise, the paragraph only describes that the sender is allowed to send a secure email, having authenticated. There is no suggestion whatsoever that the sender or the client retrieve a stored client identifier from a database.

Claims 26 and 63: The Examiner relies on Olkin, ¶ 0043 as teaching "wherein said server side database serves a plurality of services." Applicant respectfully disagrees. The cited paragraph merely indicates that it is assumed, for the sake of discussion that the sender is registered to the security server and that the receiver is not.

Claims 27 and 64: The examiner relies on Olkin, ¶¶ 0112 and 0114 as teaching "validating said trust token; and processing request without adding incremental response latency." There is no teaching in the cited paragraphs of validating a trust token. It is clear from the foregoing claims that the trust token is a separate object from authentication credentials. Here, the cited paragraph only describes evaluation of a user password. Additionally, there is no mention whatsoever of latency in the cited paragraphs.

Claims 28 and 65: The Examiner relies on Olkin, ¶ 0112 as teaching "verifying that the user ID and a client identifier in the trust token match those presented by the client on the request." As above, there is no mention in the cited paragraph of a trust token, or of a client ID or verifying that the User ID and the trust token match those provided by the user. The paragraph simply describes prompting for the password a second time if the first provided one is incorrect. As above, the foregoing claims make it clear that the trust token is a separate object from the authentication credentials.

Claims 30 and 67: The Examiner relies on Olkin, ¶ 0140 as teaching "adding a configurable amount of incremental response latency when processing untrusted logins." There is no description here of adding a configurable (specified) amount of incremental response latency. The cited paragraph merely says that if authentication fails, the receiver is either prompted for the correct password, or the decryption process is aborted. Applicant completely fails to understand how either measure could be confused for incrementally adding response latency.

Claims 31 and 68: The Examiner relies on Olkin, ¶ 0112 as teaching "wherein untrusted logins include successful and unsuccessful logins from entities not bearing a trust token." The cited paragraph merely indicates that if the user supplies an incorrect password, the software will prompt the user for the correct password. However, if the Examiner finds that authentication credentials are the same thing as a trust token, there can be no such thing as a successful login

from an entity not bearing a trust token, because without authentication credentials, a successful login is not possible. Thus, as applicant has repeatedly pointed out, the trust token is not a user Id, or a password, or a message key or a message ID. It is an object, associated to the user and a particular client, possession of which establishes a userID/client pair as trusted.

Claims 35 and 72: The Examiner relies on Olkin, ¶ 0115 as teaching "wherein said policies are applied by a server." As applicant pointed out regarding claim 1, the Examiner has not established that there are difference policies for handling trusted logins and untrusted logins.

4. **35 U.S.C. § 103**

To establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. MPEP § 2143.

Claims 9 and 46 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Olkin in view of U.S. published application no. 2002/00052921 ("Morkel"). In view of the amendments to claims 1 and 38, the present rejection is deemed overcome. Even if the independent claims had not been amended, the present rejection would be improper because, while Morkel does describe creating a hash of a user's email, there is no teaching or suggestion in either of Morkel or Olkin of placing a hash of the userId in a trust token. Accordingly, because the combination does not teach or suggest all features of the claimed invention, the present rejection would have been improper.

Claims 10, 29, 37, 47, 66, 74-76, 78-87 and 93 stand rejected as being unpatentable over Olkin in view of U.S. published application no. 2003/0028495 ("Pallante").

Claims 10 and 47: In view of the foregoing amendments to their parent claims, the present rejection is deemed overcome. Nevertheless, Applicant has the following comments:

While Pallante describes time-stamping of documents and logs, there is no teaching or suggestion in the combination of including time stamps in a trust token. Therefore, because the combination fails to teach or suggest all elements of the claimed invention, the present rejection would have been improper, even if the parent claims had not been amended.

Claims 29 and 66: In view of the foregoing amendments to their parent claims, the present rejection is deemed overcome. Nevertheless, Applicant has the following comments:

While it is true that Pallante teaches that X509 certificates have validity periods, Applicant respectfully disagrees that Pallant teaches that a trust token is a certificate. Applicant has diligently searched the reference and the only mention of a token in connection with an X509 certificate is that the key associated to the certificate can be saved to a token, such as a smart card. (¶ 0100)

Claims 37 and 74: In view of the foregoing amendments to their parent claims, the present rejection is deemed overcome. Nevertheless, Applicant has the following comments:

As above, there is no teaching or suggestion in Pallante that a trust token may be a certificate.

Claim 75: The Examiner relies on ¶ 0079 of Olkin as teaching or suggesting:

"for each successful authentication, adding or updating a database record containing at least a user identifier, an originating network address and a date/timestamp of first and/or the current successful authentication;

comparing all subsequent authentication requests to said record; and

where the user identifier of a subsequent request matches that of a

successful authentication, extending trust to the subsequent request if its originating network address satisfies predetermined criteria in relation to said record."

Applicant respectfully disagrees. The cited paragraph describes the sending of a secure email message, which, as Olkin describes, requires a successful authentication, and the creation of a receiver record for each email that is sent. The receiver record contains destination data for the message sent, which destination data, it appears, is the receiver's email address.

However, Applicant is at a complete loss to understand how the Examiner has concluded that the record created includes the originating network address. It is not stated that the message record contains the sender's email address. However, even if it were so stated, the sender's email address has nothing to do with the originating network address, which actually indicates the network location of the specific client from which the request originates. As applicant has previously explained, an email address is not an address at all but an account designator which is associated to the user and contains no information at all regarding the actual originating address of the request.

Pallante adds nothing to Olkin to teach or suggest an "originating network address." Accordingly, because the combination fails to teach or suggest all elements of the claimed invention, the present rejection is deemed improper.

In view of their dependence from an allowable parent, the dependent claims are deemed allowable without any separate consideration of their merits. Nevertheless, Applicant provides the following remarks regarding the dependent claims:

Claim 76: The Examiner relies on Olkin, ¶¶ 0047-0047 as teaching or suggesting "creating a new record by said network service if an entity has not previously authenticated to said network service; and updating a previously created record for subsequent authentication requests from said entity." While the cited paragraphs do describe creation of a new record for a receiver that has not previously authenticated to the server, there is no teaching or suggestion in the

cited paragraphs that an existing record is updated with each successful authentication.

Claim 78: The Examiner relies on Pallante, ¶ 0156 as teaching or suggesting "extending trust if the user identification and originating network address match those of the record exactly, and wherein the data/timestamps from the record satisfy configurable bounds checks." Applicant respectfully disagrees. Pallante merely discusses timestamps and says nothing about user identification and origination network address.

Claim 79: The Examiner relies on Pallante, ¶ 0079 as teaching "when the user identifier of the subsequent request matches that of a record, determining a trusted address range for the user identifier from stored authentication records." Applicant cannot understand the basis for the present finding and wonders if the Examiner is instead relying on Olkin, ¶ 0079. Olkin, ¶ 0079 describes the user alias table, which lists all email addresses associated to a user. However, as Applicant has previously explained, an email address is an email account and has nothing to do with an originating network address.

Claim 80: The Examiner relies on Olkin, ¶ 0079 and Pallante ¶ 0156 as teaching or suggesting " [determining] if the originating address of the subsequent request falls within the trusted address range, and

determining if the data/timestamps for the trusted address range satisfy configurable bounds checks." As above, Olkin does describe a plurality of email address, but an "originating network address" does not read on an email address for reasons previously explained.

Claim 83: The Examiner relies in Olkin, ¶ 0046 as teaching or suggesting "wherein the entity comprises a user requesting the network service from an anonymous client." Applicant respectfully disagrees. The cited paragraph describes that a receiver must register before they can receive secure email, however there is no teaching or suggestion that the user is requesting network service from an anonymous client.

Claim 87: The above remarks regarding claims 1 and 38 are equally applicable to claim 87.

Claim 93: The Examiner relies on Olkin as teaching "wherein said policies are applied by a server. " As described above with regard to claims 1, 38 and 87, Olkin does not teach application of different policies.

Claims 32-33, 36, 69-70 and 73 stand rejected as being unpatentable over Olkin in view of United States published application no 2002/0042883 ("Roux"). Applicant respectfully disagrees. In view of the foregoing remarks, the present rejection is deemed to be one or both of improper/overcome. Nevertheless, Applicant contributes the following remarks:

Claim 32 : The Examiner relies on Roux, ¶ 0047 as teaching "wherein response latency is added to a configurable percentage of successful untrusted logins." The cited paragraph has nothing to do with adding response latency, or adding response latency to a configurable number of logins, or adding response latecy to successful logins.". One skilled in the art would understand from the language of claim 32 that trusted logins are processed at a different rate than untrusted logins, although both the trusted logins and the untrusted logins are successful. Roux describes nothing of the sort. Roux merely says that any network request must be accompanied by a valid profile, otherwise, the request is denied. There is no mention, as the Examiner asserts of "a valid time period." There is no configurable percentage of successful trusted logins. In Roux, there are network requests accompanied by a valid profile, and those not providing a valid profile. Only request providing a valid profile are sucessful. Those not providing a valid profile are denied access (Roux, ¶ 0047, lines 12-19). There is no teaching in Roux of untrusted successful login.

Claims 33 and 70: The Examiner relies on Roux, ¶ 0047 as teaching "adding a configurable amount of incremental response latency when processing requests

from untrusted IP addresses that have exceeded a configurable login rate." Applicant respectfully disagrees. As Applicant described above, Roux has nothing to do with response latency, particularly not incremental response latency, nor does Roux have anyting to do with processing requests from untrusted IP address that have exceeded a particular login rate. "

Claims 36 and 73: The Examiner relies on Roux, ¶ 0037 as teaching "The method of claim 35, wherein said server applies rate policies for a plurality of network devices." Applicant believes the Examiner intended to type "¶ 0047." As Applicant has already explained, Roux has nothing to do with rate limiting or rate policies. It is true that Roux's server applies a policy of denying network requests that are not accompanied by a valid profile. However, this is only a single, not multiple polices, and it has nothing to do with rate or rate limiting.

Claim 69: The Examiner relies on Roux, ¶ 0047 as teaching "wherein response latency is added to a configurable percentage of successful logins." Applicant respectfully disagrees. The above remarks regarding claim 32, 33 and 36 apply equally here.

Claim 34 and 71 stand rejected as being unpatentable over Olkin in view of United States published application no. 2002/0073339 ("Card"). Applicant respectfully disagrees. In view of the foregoing, the present rejection is deemed one of both of improper/overcome.

Claim 34: The Examiner relies on Card, ¶ 0043 as teaching "wherein processing remaining requests according to at least a second policy comprises requiring an untrusted entity to complete a Turing test." Applicant respectfully disagrees. Card simply describes conventional challenge-response authentication wherein the user is asked to provide information that no one else knows. However, a Turing test does not involve provision of information that no one else knows. As known in the art, a Turing test attempts to filter machine-generated requests,

such as by cracking software, or during a DOS attack by presenting a challenge that can only be performed by humans and not by machines.

Claims 77, 88-91 and 94 stand rejected as being unpatentable over Olkin in view of Pallante and further in view of Roux. In view of the foregoing, the present rejection is deemed improper/overcome in the alternative. Nevertheless, Application provides the following remarks:

Claim 77: The Examiner relies on Roux, ¶ 0043 as teaching" wherein a network address comprises an IP (internet protocol) address." The Examiner's rationale is that "Roux teaches that if the IP address is authenticated, it adds a stronger mean of authentication when used in combination with other factors." However, Applicant can find no such teaching in Roux, ¶ 0043. Applicant respectfully requests that the Examiner point out specifically where such teaching is to be found. Applicant acknowledges that Roux does mention an IP client.

Even if Roux were to contain such teaching, Roux offers no support for the Examiner's position. In the rejection of claim 75, the Examiner found that the originating network address was an email address. Now she finds that the originating network address is a network address of an IP client. They can't be both. While it may be possible to obtain the IP address of the server hosting the user's email account, such information would certainly not yield the IP address of the client originating the request.

Claim 88: The above remarks regarding claims 33-36 are equally applicable here.

Claim 89: As above, it is incorrect that Roux teaches that untrusted logins include both successful and unsuccessful logins. As above, in Roux, there is no such thing as a successful untrusted login. An untrusted request as described by Roux is always denied.

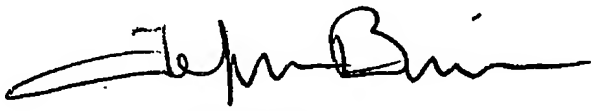
Claims 90-94: The above remarks regarding claims 33-36 are equally applicable here.

As Applicant has pointed out above, the Examiner makes several assertions regarding the teachings of the prior art for which Applicant can find no support in the references themselves. Applicant respectfully requests that the Examiner carefully review the references in question, pointing out where in references the assertions find support, also providing a detailed explanation of the rationale employed in applying the reference teachings to the claims.

CONCLUSION

In view of the foregoing, the Application is deemed to be in allowable condition. Therefore, Applicant respectfully requests reconsideration and prompt allowance of the claims. Should the Examiner have any questions regarding the Application, he is urged to contact Applicant's Attorney at 650-474-8400.

Respectfully submitted,



Jeffrey Brill
Reg. No. 51,198

Customer No. 22,862